REMARKS

Claims 1, 3-18, 20-27, 31, and 32 are currently pending in the subject application and are presently under consideration. Claims 1, 17, 18, 27 and 31 have been amended and claim 19 cancelled as shown on pages 2-6 of the Reply.

Applicants' representative thanks the Examiner for the courtesies extended during the teleconference of August 5, 2008.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 27 and 31-32 Under 35 U.S.C. §101

Claims 27 and 31-32 stand rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. Withdrawal of this rejection is requested for the following reasons. Independent claims 27 and 31 have been amended herein, and in view of this, the rejection is believed to be moot and should be withdrawn.

II. Rejection of Claims 1, 3-17, and 31-32 Under 35 U.S.C §112

Claims 1, 3-17, and 31-32 stand rejected under 35 U.S.C §112, first paragraph, as failing to comply with the enablement requirement. Withdrawal of this rejection is requested for the following reasons. Independent claims 1 and 31 have been amended herein and in view of this, the rejection is believed to be moot and should be withdrawn.

III. Rejection of Claims 1, 6-15, 17, 27, and 31-32 Under 35 U.S.C. §103(a)

Claims 1, 6-15, 17, 27, and 31-32 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Brainard (SecurSight: An Architecture for Secure Information) in view of Hypponen (US 6,986,050 B2) further in view of Bathrick *et al.* (US 5,825,300). Withdrawal of this rejection is requested for the following reasons. Brainard, Hypponen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

The claimed invention relates to a system and methodology to facilitate secure network communications between remote network entities or parties to a transaction. In particular, independent claim 1 recites *a wrapper that packages credentials associated with resources of a*

service; and a cryptographic wrapping key generated from a pass-phrase, ***the cryptographic wrapping key utilized to generate the wrapper that encapsulates the credentials, the pass-phrase employed to facilitate access to the credentials, the credentials employed to provide encrypted communication between a remote user and the service that facilitates access to the resources of the service,*** *and the pass-phrase distributed separately from the credentials.* Independent claims 27 and 31 recite similar features. Brainard, Hypponen and Bathrick *et al.*, individually or in combination, fail to teach or suggest such novel features recited by the subject claims.

Brainard relates to an architecture that secures access to network resources, while providing a smooth migration path from legacy authentication and authorization methods to a public key infrastructure. At the cited portions, Brainard discloses a personal security device (PSD) comprising a user's authentication credentials such a private key, corresponding public key certificate and other attributes. The private key of the user is encrypted and enclosed in the PSD, the private key is utilized to provide a secure connection to protected resources and perform client side authentication for the SSL session to connect to the resource. Brainard further discloses encrypting the user credentials and enclosing it in the privilege attribute certificate (PAC) along with the access controls utilized to access the resources of the service. However, Brainard discloses *two distinct credentials*, the private key in the PSD, to facilitate communication between the remote user and the service that facilitates access to the resources of the service and the access controls in the PAC that allow access to the service. Brainard also does not disclose providing encrypted communication between the service and the user. In contrast, the claimed invention provides for a single set of credentials associated with the resource, wrapped in a wrapper that is generated from a cryptographic wrapping key, the credentials employed to provide encrypted communication between the user and the service. Thus, Brainard is silent regarding ***the credentials employed to provide encrypted communication between a user and the service that facilitates access to the resources of the service*** as recited by independent claim 1. Brainard also is silent regarding ***the cryptographic wrapping key utilized to generate the wrapper that encapsulates the credentials*** as recited by amended independent claim 1. At page 6 of the Office Action, the Examiner concedes that Brainard does not disclose a cryptographic wrapping key generated from a pass-phrase, the pass-

phrase employed to facilitate access to the credentials. The Examiner attempts to compensate for the aforementioned deficiencies of Brainard with Hypponen and Bathrick *et al.*

Hypponen discloses a method of securing data stored in an electronic device comprising encrypting the data using a cryptographic key. At the cited portions of col. 3 lines 35-65, Hypponen discloses a method of preventing unauthorized access to electronic data stored in a computer device by generating a cryptographic key from a user input passphrase, storing the cryptographic key in memory and using it to encrypt and decrypt data, and allowing the user access to the encrypted data only upon receiving a password or the passphrase. Further at the cited portions of col. 3, lines 15-25, Hypponen discloses the cryptographic key derived directly from the passphrase or alternatively being encrypted using the passphrase. Thus, Hypponen discloses a passphrase that is used to generate/access a cryptographic key that facilitates encrypting and decrypting data stored in the device, where the passphrase is employed to access the device resources. In contrast, the claimed invention generates a cryptographic wrapping key from the pass-phrase, and this key is employed to *generate the wrapper*, the wrapper is employed to encapsulate the credentials. The passphrase is employed to facilitate access to the credentials employed to provide encrypted communication between a user and the service that facilitates access to the resources of the service. Thus, Hypponen is silent regarding ***the cryptographic wrapping key is utilized toe generate a wrapper that encapsulates the credentials, the pass-phrase employed to facilitate access to the credentials, the credentials employed to provide encrypted communication between a user and the service that facilitates access to the resources of the service*** as recited by the subject claims.

Bathrick *et al.* discloses computer security systems and a protected distribution of certificate and keying material between a certification authority and at least one entity in the certification authority's domain. At the cited portions, Bathrick *et al.* discloses a certifying authority that generates keying material, which includes a password and sends it to the subject entity via manual courier or other means that is different from the communication system operating through a network. However, Bathrick *et al.* does not cure the aforementioned deficiencies of Brainard and Hypponen with respect to independent claim 1.

In view of the above, Brainard, Hypponen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

Accordingly, it is respectfully submitted that this rejection be withdrawn with respect to independent claim 1(and the claims that depend there from).

IV. Rejection of Claim 16 Under 35 U.S.C. §103(a)

Claim 16 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Brainard in view of Hypponen) further in view of Bathrick *et al.* further in view of Kay *et al.* (US 6,993,555 B2). Withdrawal of this rejection is requested for the following reasons. Claim 16 depends from independent claim 1. As discussed *supra*, Brainard, Hypponen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every feature recited in independent claim 1. Kay *et al.* relates to a system for autonomously processing requests from remotely located users, using an instant messaging protocol, and does not make up for the deficiencies of Brainard, Hypponen, and Bathrick *et al.* with respect to independent claim 1. Accordingly, it is respectfully submitted that this rejection with respect to independent claim 1(from which claim 16 depends) be withdrawn.

V. Rejection of Claims 3-5 Under 35 U.S.C. §103(a)

Claims 3-5 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Brainard in view of Hypponen further in view of Bathrick *et al.* further in view of Rahman *et al.* (US 7,114,080 B2). Withdrawal of this rejection is requested for the following reasons. Claims 3-5 depend from independent claim 1. As discussed *supra*, Brainard, Hypponen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every feature recited by independent claim 1. Rahman *et al.* relates to a system that employs multiple computers outside a firewall and a password scheme that includes a one-time password and has biometric features, and does not make up for the deficiencies of Brainard, Hypponen, and Bathrick *et al.* with respect to independent claim 1. Accordingly, it is respectfully submitted that this rejection with respect to independent claim 1(from which claims 3-5 depend from) be withdrawn.

VI. Rejection of Claims 18 and 20-26 Under 35 U.S.C. §103(a)

Claims 18 and 20-26 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Hypponen in view of Brainard (SecurSight: An Architecture for Secure Information) further in view of Bathrick *et al.* Withdrawal of this rejection is requested for the following reasons.

Hypponen, Brainard and Bathrick *et al.*, alone or in combination, do not teach or suggest each and every element recited by the subject claims.

The claimed subject matter relates to a method to facilitate a security connection between remote entities. Amended independent claim 18 recites *a method to facilitate a security connection between remote entities, comprising: generating a strong password via a random generation function associated with a standard platform; generating a human-readable pass-phrase; deriving a wrapping key from the pass-phrase;* ***wrapping the password cryptographically via the pass-phrase,*** *wherein the wrapping key facilitates in encapsulating the password in a wrapper; storing the wrapped password in an executable; and transmitting the executable and the pass-phrase to a remote user system separately via different communications mediums, wherein* ***the remote user employs the pass-phrase to unlock the strong password stored in the executable, the strong password employed to establish a trust relationship with an entity.*** Hypponen, Brainard and Bathrick *et al.*, individually or in combination, fail to teach or suggest such novel features recited by the subject claims.

Hypponen discloses a method of securing data stored in an electronic device comprising encrypting the data using a cryptographic key. At pages 13-14 of the Office Action, the Examiner concedes that Hypponen does not disclose novel features of wrapping the password cryptographically via the pass-phrase, wherein the wrapping key facilitates in encapsulating the password in a wrapper.

Brainard relates to an architecture that secures access to network resources. On page 14 of the Office Action, the Examiner contends that Brainard discloses the feature of wrapping the password cryptographically via the pass-phrase. At the cited portions, Brainard discloses a user's password stored in a personal security device (PSD)/privilege attribute certificate (PAC), the PSD/PAC locked with a static password. However, the cited portion of Brainard does not disclose ***wrapping the password cryptographically via the pass-phrase*** as recited by independent claim 18. Further, at the cited portions, Brainard discloses a private key encrypted with a key-encrypting key (KEK), stored along with the KEK and password in the PSD. However, Brainard fails to disclose the password stored in the PSD being utilized to establish a trust relationship. Rather, Brainard discloses a user decrypting the private key with the stored KEK, the private key facilitates a secure connection to protected resources. In contrast, the claimed invention provides for a pass-phrase used to generate a cryptographic key that generates

a wrapper, the password encapsulated in a wrapper, a remote user using the pass-phrase to unwrap the password, and the password employed to establish a trust relationship with an entity. Thus, Brainard is silent regarding *wherein* ***the remote user employs the pass-phrase to unlock the strong password stored in the executable, the strong password employed to establish a trust relationship with an entity*** as recited by independent claim 18.

Bathrick *et al.* discloses computer security systems and a protected distribution of certificate and keying material between a certification authority and at least one entity in the certification authority's domain. At the cited portions, Bathrick *et al.* discloses a certifying authority that generates keying material, which includes a password and sends it to the subject entity via manual courier or other means that is different from the communication system operating through a network. However, Bathrick *et al.* does not cure the aforementioned deficiencies of Hypponen and Brainard with respect to independent claim 18.

In view of the above, Hypponen, Brainard and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. Accordingly, it is respectfully submitted that this rejection with respect to independent claim 18(and the claims that depend from) be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP319US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731